DEFINIÇÃO

Conceitos básicos de segurança da informação, tipos de segurança e controle de acesso.

PROPÓSITO

Apresentar os conceitos de segurança da informação e os tipos de segurança, assim como a aplicação deles.

OBJETIVOS

MÓDULO 1

Empregar os conceitos básicos da área de segurança e informação, assim como seu valor, sua propriedade e seu ciclo de vida

MÓDULO 2

Formular segurança física, lógica e controle de acesso

MÓDULO 1

Empregar os conceitos básicos da área de segurança e informação, assim como seu valor, sua propriedade e seu ciclo de vida

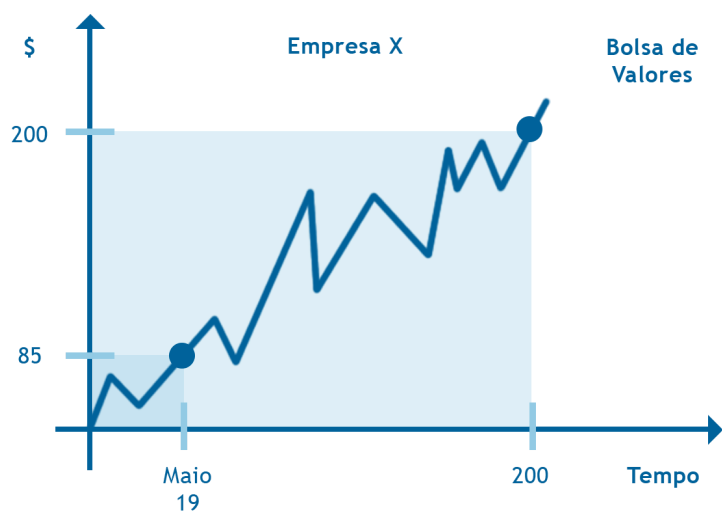
DADO E INFORMAÇÃO

As primeiras figuras rupestres datam de mais de 70 mil anos antes de Cristo. Dos manuscritos do Mar Morto até o último livro disponibilizado pela Amazon, a humanidade sempre precisou armazenar seus conhecimentos de alguma forma.

Isso nos remete ao conceito de conhecimento – ou, mais especificamente, de **informação**. Já o conceito fundamental que dá origem à informação é o **dado**.

Mas como podemos defini-lo?

O dado pode ser considerado o valor de determinada medida sem uma contextualização e, portanto, sem valor para ser aplicado ou tratado. No momento em que um dado é contextualizado, ou seja, é atribuído a um contexto ou a uma situação, torna-se uma informação, consequentemente obtendo valor.

Consideremos, por exemplo, o gráfico de uma empresa na Bolsa de Valores. Na abscissa, ele apresenta o eixo temporal; na ordenada, o valor da ação na Bolsa.

Fonte: YDUQS

Suponhamos que ela tenha registrado um crescimento durante a pandemia gerada pelo Covid-19. O valor das ações desta empresa praticamente dobrou na Bolsa de Valores.

Analisemos agora estas duas situações:

SITUAÇÃO 1

Em meados de maio de 2019, o valor da ação girava em torno de US$85; um ano depois, ele já era aproximadamente de US$200. Isso significa um aumento de mais de 100%.

SITUAÇÃO 2

Coloquemos agora tais valores em determinado contexto: suponhamos que, em meados de dezembro de 2019, fossemos informados dos dois valores dessa ação registrados nos meses de maio de 2019 e 2020.

Normalmente, uma situação do tipo não ocorre. Afinal, é muito difícil existir uma valorização tão grande em um curto espaço de tempo.

Na **situação 1**, os valores US$85 e US$200 são dados – e não contextualizados. Portanto, não é possível auferir ganhos financeiros ou elaborar uma percepção monetária a respeito deles. Mesmo que o maior *expert* em investimentos da Bolsa de Valores tivesse ciência de ambos, ele nada poderia fazer para lucrar com tais dados.

Na **situação 2**, esses valores são dados contextualizados; por isso, conhecê-los configuraria uma informação passível de se auferir ganhos monetários.

OBSERVANDO O EXEMPLO APRESENTADO, COMO PODEMOS DEFINIR UMA INFORMAÇÃO?

RESPOSTA

RESPOSTA

Ela pode ser definida como um dado contextualizado no qual existe uma percepção de valor. Dessa forma, é necessário haver uma atenção quanto à sua preservação.

CICLO DE VIDA DA INFORMAÇÃO

Por se tratar de um dado contextualizado, a informação possui o seguinte ciclo de vida:

CRIAÇÃO

TRANSPORTE

MANUSEIO

DESCARTE

Após a primeira etapa (criação), o dado pode ser transportado ou manuseado. Esta figura representa o transporte antes do manuseio por tal procedimento ser o mais comum nesses casos, porém é perfeitamente possível que ele seja manuseado anteriormente. Na etapa final, a informação é descartada.

Durante todas essas etapas, a informação deve ser protegida. Seu vazamento em quaisquer etapas pode provocar problemas em vários aspectos.

Vamos analisar alguns exemplos disso:

1º

Transporte inadequado de dados por uma transportadora que não realiza todos os procedimentos de segurança necessários.

Um *laptop* é levado para a manutenção sem que os dados do disco rígido dele sejam protegidos. Não é raro haver casos de roubos de unidades que possuíam informações sensíveis de empresas.

Fonte: (FREIRE, 2008)

2º

3º

Um analista de dados tem um *laptop* e um disco rígido externo roubados em sua residência com informações não criptografadas de 26,5 milhões veteranos do exército americano. O analista informou que **rotineiramente** levava os dados para a sua residência. Neste caso, o problema ocorreu no manuseio da informação.

Fonte: (GUSMÃO, 2014)

Empresa forense de Nova Iorque, a Kessler International realizou o seguinte estudo: durante seis meses, ela foi adquirindo discos rígidos usados no portal eBay. Cerca de 40% deles continham informações de seus usuários.

Fonte: (MEARIAN, 2009)

4º

5º

Exemplos simples e clássicos como os apresentados acima não correspondem apenas a empresas que não sejam de tecnologia da informação (TI). Até mesmo o Facebook, uma das companhias mais novas do mercado de tecnologia e com um altíssimo valor agregado, sendo usado por milhões de pessoas no mundo, teve um disco rígido furtado de um veículo. Ele continha informações de aproximadamente 29.000 empregados norte-americanos.

Fonte: (BE COMPLIANCE, 2019)

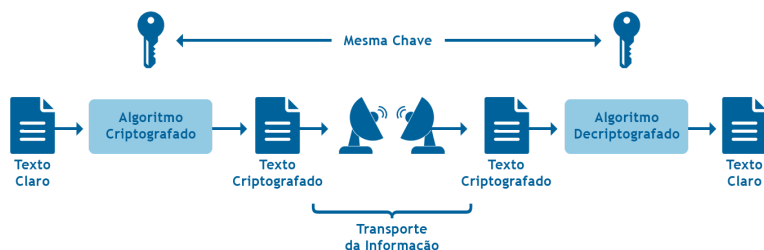
Que conclusão podemos tirar dos casos apresentados?

A informação, que é o dado contextualizado, precisa de proteção em todo o seu ciclo de vida. A partir dos exemplos citados, conseguimos entender a necessidade de **sempre** estabelecer uma proteção adequada dela em qualquer etapa do seu ciclo de vida.

No caso do transporte de mídias magnéticas contendo informações sigilosas de usuários de determinada empresa, por exemplo, uma boa proteção é o emprego da **criptografia**. Esta chave é usada para embaralhar (criptografar) e desembaralhar (decriptografar) as informações.

Quando a mesma chave é usada nas duas etapas, a criptografia é dita **simétrica**; quando são usadas chaves distintas, ela é **assimétrica**. Vejamos seus dois tipos nas figuras a seguir:

CRIPTOGRAFIA

Ela pode ser definida como o embaralhamento das informações por meio de uma sequência de dados que utiliza uma chave e um algoritmo.

Fonte: YDUQS

CRIPTOGRAFIA SIMÉTRICA.

Fonte: YDUQS

CRIPTOGRAFIA ASSIMÉTRICA.

Como você manuseia seu *pen drive*?

Hoje em dia, por estarmos na era da informação, é comum sempre levarmos um desses dispositivos no bolso, mochila ou na carteira.

Afinal, como você cuida das suas informações?

Certamente, seu *pen drive* contém alguns arquivos nos quais você ainda deve estar trabalhando. Ele pode servir para várias pessoas e diferentes tipos de trabalho:

Se você é um programador, pode estar mexendo em alguma parte de um sistema que está desenvolvendo;

Se você trabalha na direção, pode estar atualizando alguma planilha com os dados financeiros da sua empresa.

Uma prática simples – mas eficiente – nestes casos é simplesmente compactar os seus arquivos usando uma senha.

Fonte: YDUQS

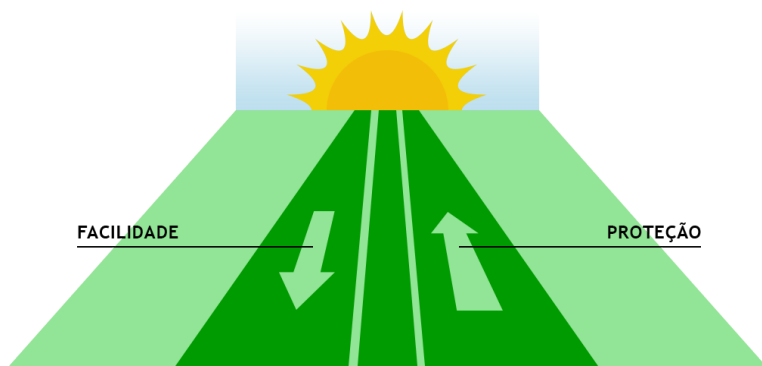
ARQUIVOS NO *PEN DRIVE* SEM SENHA.

Fonte: YDUQS

ARQUIVO COMPACTADO CONTENDO TODOS OS ARQUIVOS COM SENHA.

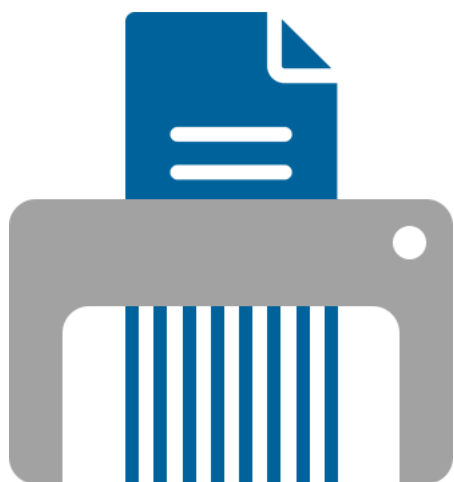
Praticamente todas as ferramentas (até mesmo as gratuitas) possuem essa funcionalidade. Cada uma conta com uma metodologia para acrescer a senha ao processo de compactação. Um bom exemplo disso é a ferramenta 7-zip.

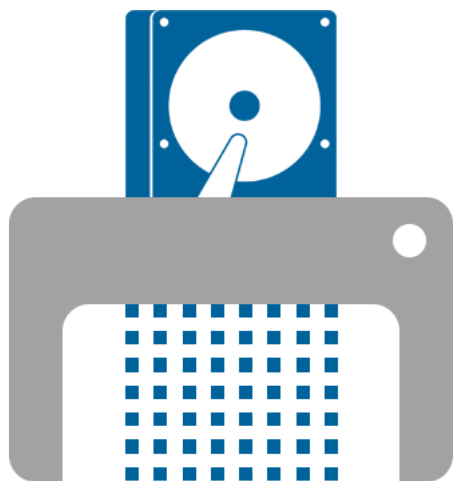
Essas ferramentas utilizam os melhores algoritmos de criptografia existentes no mercado. Além de economizar o espaço do *pen drive*, essa simples prática cria ainda uma camada de proteção para as informações contidas no dispositivo.

Devemos observar que a **proteção** e a **facilidade** caminham em direções contrárias. Por isso, o processo de compactar com senha gera um aumento de tempo no manuseio da informação, pois ele sempre torna necessária a tarefa de descompactar e compactar para tratar a informação.

Fonte: YDUQS

A proteção e a facilidade sempre caminham em sentidos opostos.

Dessa forma, seu descarte deve ser realizado de forma padronizada, já que o propósito é evitar a recuperação de suas informações. Exemplo: *pen drives*, discos rígidos e outras mídias usadas precisam ser descartadas com o uso de trituradores adequados.

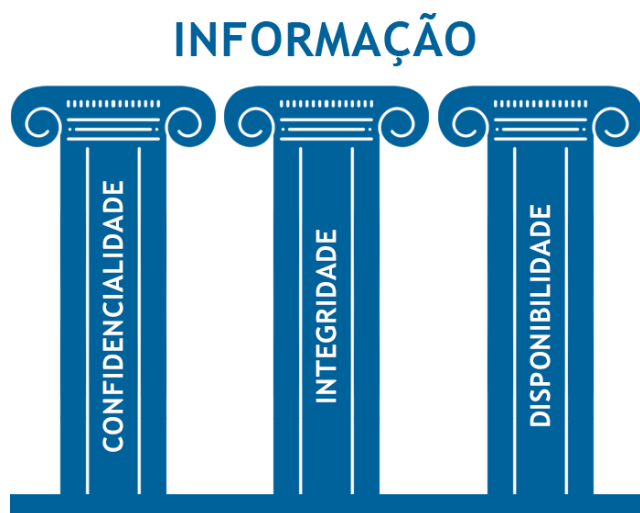
Nas figuras a seguir, exibiremos dois tipos de trituradores:

Fonte: YDUQS

TRITURADOR DE PAPEL.

Fonte: YDUQS

TRITURADOR DE DISCO RÍGIDO.

ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

Dos aspectos da informação, seus três principais requerem cuidados especiais:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Fonte: YDUQS

Principais pilares da informação: confidencialidade, integridade e disponibilidade.

Confidencialidade

Capacidade do acesso à informação apenas por quem possui autorização.

Integridade

Possibilidade de alteração da informação por pessoas ou sistemas autorizados.

Disponibilidade

Faculdade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

Citados por diversos autores como pilares, estes três aspectos, conforme indica a imagem acima, correspondem à prioridade do que deve ser protegido em relação à informação. Todos os exemplos citados correspondem, portanto, à confidencialidade da informação em três momentos diferentes do seu ciclo de vida.

Portanto, a **segurança da informação** pode ser definida como as atividades, os procedimentos e as metodologias que objetivam a proteção da informação, principalmente no que tange à confidencialidade, à integridade e à disponibilidade (CID).

Os seguintes aspectos, contudo, também são considerados importantes:

Fonte: YDUQS/Shutterstock

AUTENTICIDADE

Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

Fonte: YDUQS/Shutterstock

LEGALIDADE

Trata-se do alinhamento da informação e/ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos, cada um na sua respectiva esfera de atribuição e abrangência.

Fonte: YDUQS/Shutterstock

NÃO REPÚDIO

Também conhecido como **irretratabilidade**, ele está relacionado ao fato de o emissor negar a autoria de uma informação divulgada.

Juntos, todos eles compõem os principais aspectos empregados pelos controles – ou pelas ferramentas que proporcionam a segurança da informação – para proteger a informação.

Resumo dos aspectos da segurança:

D	V	F	T	Y	H	E	A	C	V	D	A	D	E	A	Z	C	U	I	O	K
A	D	E	D	A	D	D	A	D	E	D	A	D	E	D	A	**D**	D	A	D	E
E	R	E	D	V	F	T	Y	H	E	A	C	V	D	A	D	**I**	A	C	V	D
D	A	D	A	D	E	D	A	D	D	A	D	E	D	A	D	**S**	D	A	D	V
A	C	V	A	A	A	C	V	S	A	C	V	D	D	A	D	**P**	D	V	F	D
S	V	F	T	Y	H	E	A	C	V	D	A	D	D	V	F	**O**	V	D	V	D
P	D	E	D	A	D	D	A	D	E	D	A	D	A	D	E	**N**	D	F	D	A
O	S	E	D	V	A	T	Y	H	E	A	C	V	D	A	D	**I**	F	A	F	A
N	P	D	A	A	V	D	A	D	D	A	D	E	D	A	D	**B**	A	E	A	V
R	O	S	A	V	D	**I**	**R**	**R**	**E**	**T**	**R**	**A**	**T**	**A**	**B**	**I**	**L**	**I**	**D**	**A**

A	N	P	V	D	A	F	T	Y	H	F	T	Y	H	A	S	**L**	F	T	Y	H
D	R	O	D	A	Y	E	D	A	D	E	D	A	D	Z	C	**I**	E	D	A	D
C	A	N	A	Y	A	F	T	Y	H	A	**C**	**O**	**N**	**F**	**I**	**D**	**E**	**N**	**C**	**I**
D	D	R	Y	A	V	E	D	A	D	S	F	G	H	J	K	**A**	Q	W	E	R
A	D	A	A	V	D	A	**A**	**U**	**T**	**E**	**N**	**T**	**I**	**C**	**I**	**D**	**A**	**D**	**E**	D
A	C	D	V	D	T	Y	H	F	T	Y	H	E	A	A	A	**E**	F	T	Y	D
A	D	D	D	F	T	Y	H	F	T	Y	H	E	A	C	V	D	E	D	A	E
V	D	C	P	E	D	A	D	E	D	A	D	D	A	D	E	D	A	D	Q	D
E	D	D	O	A	A	C	V	A	A	A	C	V	D	A	D	E	D	A	D	C
C	V	A	N	F	T	Y	H	V	F	T	Y	H	E	A	C	V	D	A	D	D
D	E	A	D	E	D	A	D	D	E	D	A	D	D	A	D	E	D	A	D	A
E	D	D	O	A	A	B	D	E	D	D	O	A	A	C	V	A	A	A	C	V
C	V	A	N	F	T	A	A	C	V	A	N	F	T	Y	H	V	F	T	Y	H
D	E	A	D	E	D	Q	A	D	E	A	D	E	D	A	D	D	E	D	A	D

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

DISPONIBILIDADE

Capacidade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

IRRETRATABILIDADE

Está relacionada ao emissor negar a autoria de uma informação divulgada.

CONFIDENCIALIDADE

Capacidade do acesso à informação apenas por quem possui autorização.

AUTENTICIDADE

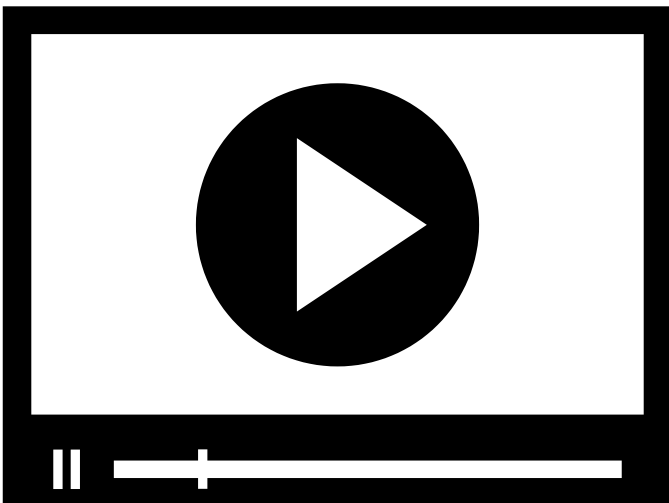
Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

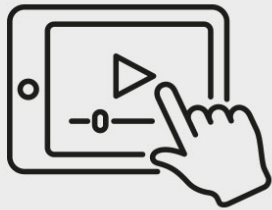
INTEGRIDADE

Possibilidade de alteração da informação por pessoas ou sistemas autorizados.

LEGALIDADE

Alinhamento da informação ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos.

Palavras cruzadas dos aspectos da segurança.

Neste vídeo, empregaremos os conceitos básicos da área de segurança e informação, citando seu valor, propriedade e ciclo de vida.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

MÃO NA MASSA

1) (2019 - INSTITUTO UNIFIL - PREFEITURA DE CAMBÉ/PR - PSICÓLOGO) A SEGURANÇA DA INFORMAÇÃO ESTÁ RELACIONADA À PROTEÇÃO DE UM CONJUNTO DE DADOS NO SENTIDO DE PRESERVAR OS VALORES QUE POSSUEM PARA UM INDIVÍDUO OU UMA ORGANIZAÇÃO. O CONCEITO SE APLICA A TODOS OS ASPECTOS DE PROTEÇÃO DE INFORMAÇÕES E DADOS. O CONCEITO DE SEGURANÇA INFORMÁTICA OU SEGURANÇA DE COMPUTADORES ESTÁ INTIMAMENTE RELACIONADO COM ELE, INCLUINDO NÃO APENAS A SEGURANÇA DOS DADOS/INFORMAÇÃO, MAS TAMBÉM A DOS SISTEMAS EM SI. ASSINALE A ALTERNATIVA QUE NÃO REPRESENTA UM DOS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO.

A) Confidencialidade

B) Integridade

C) Permutabilidade

D) Disponibilidade

2) (2019 - IDECAN - IF-AM - BIBLIOTECÁRIO DOCUMENTALISTA) A SEGURANÇA DA INFORMAÇÃO ESTÁ BASEADA EM TRÊS PILARES: CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE. COM BASE NESSA INFORMAÇÃO, ANALISE AS AFIRMATIVAS A SEGUIR.

> **GARANTIR O ACESSO POR PESSOA OU DISPOSITIVO DEVIDAMENTE AUTORIZADO A TODO *HARDWARE*, *SOFTWARE* E DADOS SEMPRE QUE NECESSÁRIO.**
>
> **AS INFORMAÇÕES DEVEM SER ARMAZENADAS DA FORMA COMO FORAM CRIADAS, DE MODO QUE NÃO SEJAM CORROMPIDAS OU DANIFICADAS.**
>
> **AS INFORMAÇÕES NÃO PODERÃO SER VISTAS OU UTILIZADAS SEM AS DEVIDAS AUTORIZAÇÕES DE ACESSO POR PESSOAS OU DISPOSITIVOS.**

ASSINALE A ALTERNATIVA QUE APRESENTE A ORDEM CORRETA DE ASSOCIAÇÃO COM OS TRÊS PILARES DA SEGURANÇA DA INFORMAÇÃO.

A) I – Disponibilidade, II – Integridade, III – Confidencialidade.

B) I – Confidencialidade, II – Integridade, III – Disponibilidade.

C) I – Integridade, II – Confidencialidade, III – Disponibilidade.

D) I – Confidencialidade, II – Disponibilidade, III – Integridade.

3) (2020 - IDIB - PREFEITURA DE COLINAS DO TOCANTINS/TO - ENGENHEIRO CIVIL) EM SE TRATANDO DE SEGURANÇA DA INFORMAÇÃO, A LITERATURA DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO ELENCA TRÊS PRIORIDADES BÁSICAS. ESSAS TRÊS

PRIORIDADES TAMBÉM SÃO CHAMADAS DE PILARES DA SEGURANÇA DA INFORMAÇÃO. ASSINALE A ALTERNATIVA QUE INDICA CORRETAMENTE O NOME DA PRIORIDADE BÁSICA QUE ESTÁ RELACIONADA AO USO DE RECURSOS QUE VISAM RESTRINGIR O ACESSO ÀS INFORMAÇÕES.

A) Inviolabilidade

B) Confidencialidade

C) Acessibilidade

D) Invulnerabilidade

4) (2019 - NC-UFPR - PREFEITURA DE MATINHOS/PR - FISCAL DE TRIBUTOS) SOBRE AS POLÍTICAS ESPECÍFICAS DE SEGURANÇA, O TERMO DE USO OU DE SERVIÇO É UM DOCUMENTO QUE DEFINE AS REGRAS DE USO DOS RECURSOS COMPUTACIONAIS, OS DIREITOS E AS RESPONSABILIDADES DE QUEM OS UTILIZA E AS SITUAÇÕES QUE SÃO CONSIDERADAS ABUSIVAS. ESSE CONCEITO SE REFERE À POLÍTICA DE:

A) Uso aceitável

B) Confidencialidade

C) Privacidade

D) Não repúdio

5) A INTERNET FOI CRIADA NO FINAL DA DÉCADA DE 1990 NOS LABORATÓRIOS DO CERN PELO FÍSICO BRITÂNICO TIM BERNS-LEE. DESDE AQUELE TEMPO, DIVERSAS CRIAÇÕES VIERAM MOLDANDO AS GERAÇÕES SUBSEQUENTES. ATUALMENTE, DESTACAM-SE AS IMAGENS NA INTERNET CONHECIDAS COMO MEMES. ALGUNS DELES TÊM, NA VERDADE, UM CARÁTER EDUCATIVO, ENSINANDO, DE FORMA LÚDICA, ALGUMAS PRÁTICAS QUE NÃO DEVEM SER SEGUIDAS. UMA DELAS É O MANUSEIO DE SENHAS.

NA VERDADE, A IDEIA É ENSINAR AO USUÁRIO A MANUSEAR SUA SENHA DE FORMA CORRETA, NÃO DEIXANDO-A, POR EXEMPLO, EMBAIXO DO TECLADO. NO MEME DO TAPETE QUE FALA SOBRE ISSO, O OBJETIVO É ENSINAR AO USUÁRIO COMO MANEJÁ-LA CORRETAMENTE. MARQUE O ITEM QUE INTEGRA ESSE ENSINAMENTO.

A) Confidencialidade

B) Disponibilidade

C) Integridade

D) Irretratabilidade

6) ALGUNS ANOS APÓS SUA APOSENTADORIA, BILL RESOLVE ESTUDAR PARA OBTER UMA CERTIFICAÇÃO DE SEGURANÇA. ELE E SEU VIZINHO DE PORTA, STEVE, QUE TAMBÉM GOSTARIA DE TIRAR A TÃO SONHADA CERTIFICAÇÃO, RESOLVEM CRIAR MNEMÔNICOS PARA DECORAR OS ASSUNTOS.

PARA DECORAR OS PILARES DA SEGURANÇA DA INFORMAÇÃO, ELES CRIAM O SEGUINTE MNEMÔNICO: “CRESCI VENDO TELEVISÃO. SEMPRE ACHEI O CID MUITO SEGURO AO NARRAR AS REPORTAGENS”. BILL E STEVE CRIARAM VÁRIOS MNEMÔNICOS. NO DIA SEGUINTE, HOUVE A PROVA DE CERTIFICAÇÃO. SUA PRIMEIRA QUESTÃO VERSAVA SOBRE OS PILARES. A IDEIA DO MNEMÔNICO DEU CERTO, MAS ELES ESQUECERAM O QUE REPRESENTAVA CADA LETRA.

VOCÊ RESOLVE EXPLICAR PARA ELES O SIGNIFICADO DE CADA UMA. MARQUE A ALTERNATIVA QUE APRESENTA OS TERMOS CORRETOS.

A) Confidencialidade, integridade e disponibilidade.

B) Confiabilidade, integridade e disponibilidade.

C) Confidencialidade, irretratabilidade e disponibilidade.

D) Confiabilidade, integridade e dedutibilidade.

GABARITO

1) (2019 - Instituto UniFil - Prefeitura de Cambé/PR - psicólogo) A segurança da informação está relacionada à proteção de um conjunto de dados no sentido de preservar os valores que possuem para um indivíduo ou uma organização. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de segurança informática ou segurança de computadores está intimamente relacionado com ele, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si. Assinale a alternativa que não representa um dos princípios da segurança da informação.

A alternativa **"C "** está correta.

Os principais pilares da segurança da informação são a confidencialidade, a integridade e a autenticidade. Há os complementares, como a autenticidade, a legalidade e o não repúdio.

2) (2019 - IDECAN - IF-AM - bibliotecário documentalista) A segurança da informação está baseada em três pilares: confidencialidade, integridade e disponibilidade. Com base nessa informação, analise as afirmativas a seguir.

Garantir o acesso por pessoa ou dispositivo devidamente autorizado a todo *hardware*, *software* e dados sempre que necessário.

As informações devem ser armazenadas da forma como foram criadas, de modo que não sejam corrompidas ou danificadas.

As informações não poderão ser vistas ou utilizadas sem as devidas autorizações de acesso por pessoas ou dispositivos.

Assinale a alternativa que apresente a ordem correta de associação com os três pilares da segurança da informação.

A alternativa **"A "** está correta.

A disponibilidade determina que seja garantido o acesso. As informações deverem ser armazenadas da forma como foram criadas vincula-se automaticamente com a integridade. A informação poder ser vista apenas por pessoas autorizadas é a confidencialidade.

3) (2020 - IDIB - Prefeitura de Colinas do Tocantins/TO - engenheiro civil) Em se tratando de segurança da informação, a literatura da área de tecnologia da informação elenca três prioridades básicas. Essas três prioridades também são chamadas de pilares da segurança da informação. Assinale a alternativa que indica corretamente o nome da prioridade básica que está relacionada ao uso de recursos que visam restringir o acesso às informações.

A alternativa **"B "** está correta.

Os pilares são confidencialidade, integridade e disponibilidade, além de autenticidade, legalidade e não repúdio.

4) (2019 - NC-UFPR - Prefeitura de Matinhos/PR - fiscal de tributos) Sobre as políticas específicas de segurança, o termo de uso ou de serviço é um documento que define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas. Esse conceito se refere à política de:

A alternativa **"A "** está correta.

Os pilares da segurança da informação são definidos por confidencialidade, integridade, disponibilidade, autenticidade e legalidade, além do não repúdio. Tais conceitos têm relação com os pilares, e não diretamente com as políticas.

5) A internet foi criada no final da década de 1990 nos laboratórios do CERN pelo físico britânico Tim Berns-Lee. Desde aquele tempo, diversas criações vieram moldando as gerações subsequentes. Atualmente, destacam-se as imagens na internet conhecidas como memes. Alguns deles têm, na verdade, um caráter educativo, ensinando, de forma lúdica, algumas práticas que não devem ser seguidas. Uma delas é o manuseio de senhas.

Na verdade, a ideia é ensinar ao usuário a manusear sua senha de forma correta, não deixando-a, por exemplo, embaixo do teclado. No meme do tapete que fala sobre isso, o objetivo é ensinar ao usuário como manejá-la corretamente. Marque o item que integra esse ensinamento.

A alternativa **"A "** está correta.

A confidencialidade está relacionada à manutenção de uma informação passível de ser observada, lida ou acessada apenas por quem tem direito. Em outras palavras, é semelhante a deixar uma conta de *e-mail* aberta para que qualquer pessoa possa lê-la sem precisar da senha (chave embaixo do tapete, senha embaixo do teclado).

6) Alguns anos após sua aposentadoria, Bill resolve estudar para obter uma certificação de segurança. Ele e seu vizinho de porta, Steve, que também gostaria de tirar a tão sonhada certificação, resolvem criar mnemônicos para decorar os assuntos.

Para decorar os pilares da segurança da informação, eles criam o seguinte mnemônico: "Cresci vendo televisão. Sempre achei o CID muito seguro ao narrar as reportagens". Bill e Steve criaram vários mnemônicos. No dia seguinte, houve a prova de certificação. Sua primeira questão versava sobre os pilares. A ideia do mnemônico deu certo, mas eles esqueceram o que representava cada letra.

Você resolve explicar para eles o significado de cada uma. Marque a alternativa que apresenta os termos corretos.

A alternativa **"A "** está correta.

C é de confidencialidade, que é a capacidade do acesso à informação apenas por aqueles que possuem autorização; I, de integridade, que é a possibilidade de alteração da informação por pessoas ou sistemas autorizados; e D, de disponibilidade, que é a faculdade de uma informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

GABARITO

TEORIA NA PRÁTICA

Todas as profissões possuem suas características. Nós, que somos de TIC, precisaremos, uma hora ou outra, interagir com elas e assegurar que tais características sejam cumpridas.

Uma das mais antigas profissões do mundo é a do médico. Aqueles que já fizeram o juramento de Hipócrates e sabem quão árdua esta profissão é estão cientes de que um de seus fundamentos é o sigilo entre médico e paciente.

Esse sigilo aparece transcrito no CFM 1605/2000 em adição ao Código de Processo Penal (1941, art. 207), que dispõe o seguinte: "São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho". Isso reforça ainda mais a necessidade de proteção desses dados não apenas quanto à confidencialidade deles, mas também em relação à sua integridade.

No tocante à confidencialidade, como os administradores de banco de dados devem fazer para gerenciá-los, uma vez que eles podem manusear quaisquer dados armazenados em um SGBD?

RESPOSTA

A resposta padrão a este questionamento cada vez mais comum é o uso de criptografia na base de dados sem que a chave (simétrica, pública ou privada) esteja em *hard code*, tampouco armazenada no BD ou no arquivo de computador.

VERIFICANDO O APRENDIZADO

1) AO REALIZARMOS O *DOWNLOAD* DE UMA ISO DE UM *SOFTWARE*, NORMALMENTE USAMOS AS FUNÇÕES DE HASH. MARQUE A ALTERNATIVA QUE APRESENTA O PILAR DA SEGURANÇA DA INFORMAÇÃO QUE CORRESPONDE AO USO DESSAS FUNÇÕES.

A) Confidencialidade

B) Integridade

C) Disponibilidade

D) Legalidade

2) CONSTITUI UM DEVER DE TODO CIDADÃO ELABORAR ANUALMENTE O IMPOSTO DE RENDA. COM O ADVENTO DA INTERNET, A NOSSA DECLARAÇÃO AGORA PODE SER ENVIADA DIRETAMENTE PARA OS SERVIDORES DO GOVERNO. NO INÍCIO DESSA METODOLOGIA, ERA COMUM HAVER NOTÍCIAS NOS TELEJORNAIS SOBRE OS SERVIDORES NÃO AGUENTARAM E SE DESLIGAREM SOZINHOS. MARQUE A ALTERNATIVA QUE APRESENTE O PILAR DA SEGURANÇA DA INFORMAÇÃO QUE DENOMINA PERFEITAMENTE TAL SITUAÇÃO.

A) Confidencialidade

B) Integridade

C) Disponibilidade

D) Conformidade

GABARITO

1) Ao realizarmos o *download* de uma ISO de um *software*, normalmente usamos as funções de hash. Marque a alternativa que apresenta o pilar da segurança da informação que corresponde ao uso dessas funções.

A alternativa **"B "** está correta.

As funções de *hash* criam um conjunto de valores alfanuméricos que representa a informação. Alterando-se um bit da informação, normalmente todo o conjunto de valores é alterado. Dessa forma, assegura-se de que não haverá alteração da informação.

2) Constitui um dever de todo cidadão elaborar anualmente o imposto de renda. Com o advento da internet, a nossa declaração agora pode ser enviada diretamente para os servidores do governo. No início dessa metodologia, era comum haver notícias nos telejornais sobre os servidores não aguentaram e se desligarem sozinhos. Marque a alternativa que apresente o pilar da segurança da informação que denomina perfeitamente tal situação.

A alternativa **"B "** está correta.

Quando os servidores foram desligados, pararam de funcionar; com isso, tornaram-se indisponíveis.

MÓDULO 2

⦿ **Formular segurança física, lógica e controle de acesso**

SEGURANÇA FÍSICA

No módulo anterior, vimos o exemplo de roubo de dados no seu transporte. Mesmo que eles estivessem criptografados, a ação poderia ocorrer da mesma forma, pois ela foi uma consequência de vulnerabilidades na segurança física das mídias em questão.

Aspecto integridade

A informação foi totalmente impactada, pois a mídia poderia ser destruída.

Aspecto confidencialidade

Dependeria, por exemplo, da informação armazenada ter ou não algum controle de proteção, como, por exemplo, a criptografia.

A família de normas ABNT ISO/IEC 27.000 divide a segurança física em dois aspectos: um é relacionado aos equipamentos e outro, ao ambiente.

A segurança da informação age dessa forma. Ela é entendida como camadas justapostas que permitem à informação ficar cada vez mais protegida, como, por exemplo, uma cebola e suas camadas.

Quanto ao ambiente, em uma instalação empresarial, por exemplo, é possível observar as camadas de segurança físicas e, a partir daí, estabelecer um paralelo com a imagem da cebola.

Fonte: YDUQS

Nossa informação deve receber camadas de proteção como se fosse uma cebola.

Ao nos aproximarmos de uma instalação, alcançamos a cancela para automóveis, que, normalmente, conta com dois seguranças. Sua função é solicitar alguma identificação ou verificar se o veículo possui algum selo de identificação.

Normalmente, esse selo é único para aquela instituição. Em alguns casos, essa verificação pode ser feita de forma automatizada com alguma tecnologia de emissão de sinal de baixa frequência, como o RFID.

Após a ultrapassagem dessa primeira barreira (camada mais externa à nossa cebola de segurança), geralmente existe mais uma etapa: catraca e elevador. Ela está vinculada a algum controle biométrico ou de crachá. O RFID novamente surge como um exemplo.

Físicos, esses controles são justapostos, permitindo que a vulnerabilidade de um deles possa ser recoberta por outro controle. Isso funciona de forma similar nas salas de servidores, *data centers* e salas-cofres, criando camadas de segurança que dificultam o acesso físico ao servidor.

Outro aspecto que deve ser levado em consideração é a proteção contra ameaças da natureza, como enchentes, incêndios e outras calamidades provocadas pela natureza e/ou pelo homem.

Tendo isso em vista, certos controles de monitoramento e prevenção devem ser instalados e controlados.

EXEMPLO

Câmeras de segurança, controles de temperatura, extintores de incêndio e *sprinkles* (algumas vezes traduzidos como chuveiros automáticos).

O cabeamento e o acesso à rede externa (internet), bem como ao fornecimento de energia, são fatores fundamentais nesse processo. Como eles dependem de um fornecimento feito por terceiros, certos aspectos contratuais e de redundância precisam ser estabelecidos.

Além disso, políticas e instruções normativas devem ser instituídas, treinadas e simuladas visando à prontidão. Nesse sentido, é razoável haver uma redundância no fornecimento de rede (internet), bem como uma independência física desse fornecimento no que tange ao tipo de conexão estipulada.

É necessário evitar o uso compartilhado de conexões entre fornecedores distintos. Desse modo, se, para um fornecedor, a conexão é feita por meio de fibra ótica, para o outro ela poderia ser realizada por intermédio de link rádio.

Sobre a parte de energia elétrica, o uso de bancos de bateria (e/ou no-breaks) e de geradores revela ser algo fundamental na maioria dos casos. Quanto aos geradores, deve-se levar em consideração o fornecimento de insumos necessários e periódicos, como o combustível.

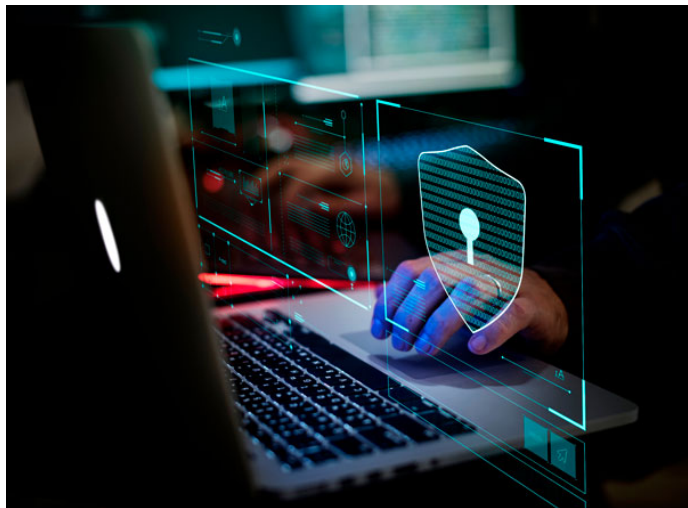
Em relação aos equipamentos, a ideia de segurança tem relação com o acesso físico aos componentes de *hardware* e aos dispositivos de entrada. Devem ser adotadas medidas como senha na BIOS e configuração de botões físicos e de ordem de execução na inicialização dos computadores.

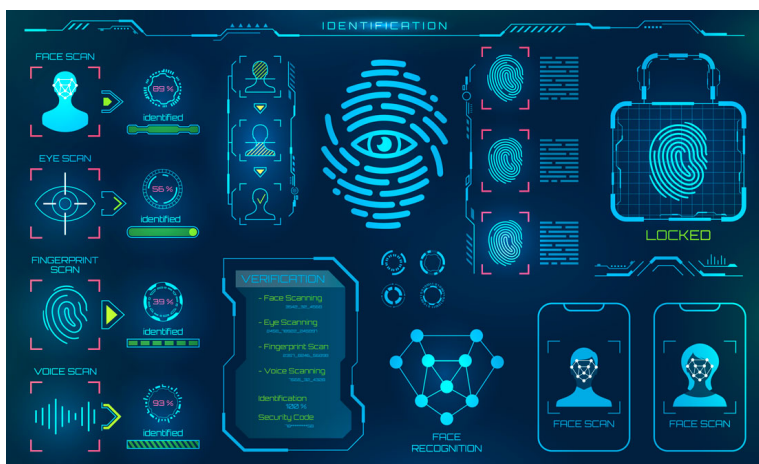
Os maiores computadores do mundo são organizados em uma lista conhecida como Top 500 (top500.org). Pelo custo e poder computacional deles, esses equipamentos requerem uma série de recursos de proteção.

Maior recurso computacional do Brasil, o supercomputador Santos Dumont consta na referida lista. Para prover os recursos necessários de segurança, uma série de medidas foi tomada e, em seguida, publicada no Youtube.

SEGURANÇA LÓGICA

Em adição às medidas de segurança física, há as de segurança lógica, que correspondem às medidas baseadas em *software.* Dessa lista, podemos destacar as senhas, as listas de controle de acesso, a criptografia, e o *firewall*.

Repetindo o padrão apresentado anteriormente, esses mecanismos estão justapostos; com isso, a demanda de uma camada pode criar uma adicional a outra que possua alguma vulnerabilidade particular.

Fonte: Rawpixel.com/Shutterstock

Como exemplo disso, existem no próprio equipamento controles de acessos biométricos, como a leitura de digital e o reconhecimento facial. Esses sistemas de controle biométricos são caracterizados pela captura da geometria humana, a qual, em grande parte, difere em cada pessoa.

Fonte: Mad Dog/Shutterstock

Atualmente, os leitores de digitais têm dado espaço para o reconhecimento facial pela disseminação dos sensores e da tecnologia empregada. Há diversas APIs disponibilizadas para uso gratuito e comercial, como a do Amazon Rekognition. Esses controles atuam na proteção da confidencialidade da informação.

A criptografia corresponde ao conjunto de técnicas que permite o embaralhamento de dados por intermédio do uso de chaves e de algoritmos computacionais baseados em funções matemáticas. Essas funções propiciam, em linhas gerais, a presença de duas grandes classes de algoritmos: os **simétricos** e os **assimétricos**.

CRIPTOGRAFIA SIMÉTRICA

Utiliza funções matemáticas mais simples e uma única chave para criptografar e decriptografar. Esta classe de algoritmos é composta por, entre outros exemplos, Cifra de César, Blowfish, Twofish e Rijnadel. Graças a esse controle, é possível assegurar a confidencialidade da informação.

Algoritmo	Tamanho da chave
AES (Rijnadel)	128, 192 e 256 bits
Twofish	128, 192 e 256 bits
Serpent	128, 192 e 256 bits
Blowfish	32 a 448-bits
RC4	40-128 bits
3DES (baseado no DES)	168 bits
IDEA	128 bits

 Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

CRIPTOGRAFIA ASSIMÉTRICA

Caracteriza-se por algoritmos que normalmente envolvem técnicas matemáticas mais sofisticadas, como a fatoração de números grandes e o logaritmo discreto.

Esta família emprega duas chaves: uma é utilizada para cifrar; a outra, para decifrar. Essas chaves são conhecidas como:

Pública

Normalmente, ela fica disponibilizada em um servidor de confiança.

Privada

Ela está sob a posse do usuário.

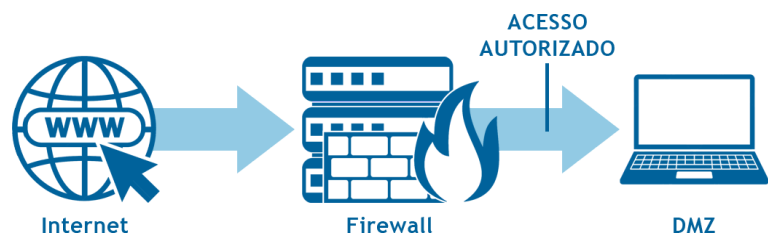
Com a combinação dessas duas chaves, é possível assegurar não somente a confidencialidade, mas também o não repúdio ou irretratabilidade. Afinal, pode-se combinar o uso desse controle tanto com a chave privada do emissor (não repúdio) quanto com a pública do destinatário (confidencialidade).

Diffie-Hellman, El Gamal e Curvas Elípticas são alguns dos algoritmos desta família. Quanto aos controles aplicados às redes, destacam-se os ***firewalls***, os sistemas detectores de intrusão e os VPNs.

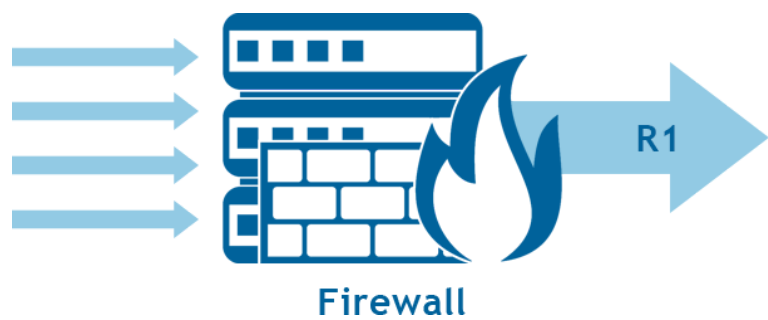
Esses controles permitem a criação de zonas de segurança dentro e fora da instituição. Tais zonas, por sua vez, possibilitam a criação de segregações de funcionalidades.

Das zonas de segurança, a mais comumente encontrada é a DMZ. Zona desmilitarizada, ela limita, conforme demonstra a figura a seguir, a região onde os servidores *web* e de aplicação podem ficar.

FIREWALLS

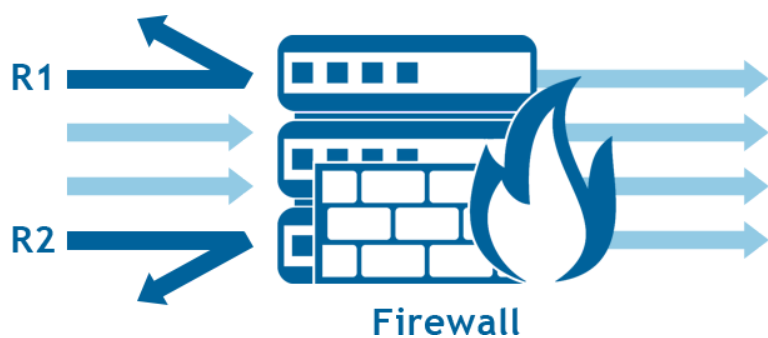
Equipamentos que filtram o tráfego de rede relacionado à troca de dados entre clientes e servidores.

Fonte: YDUQS

📷 Diagrama simplificado de uma DMZ.

As regras dos *firewalls* podem seguir duas políticas:

Fonte: YDUQS

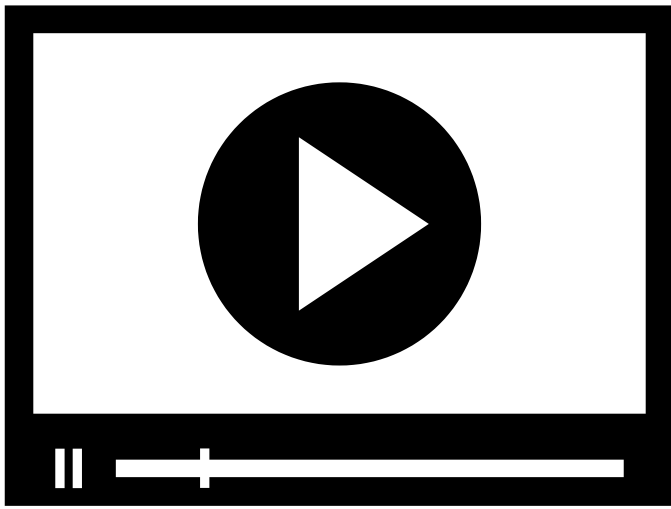
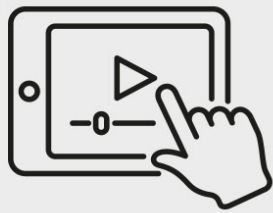
NEGAR POR PADRÃO

Todo o tráfego é negado. Apenas os servidores e os protocolos são autorizados.

Trata-se da política normalmente encontrada e recomendada no mercado. Como todos os tráfegos são negados, apenas podem trafegar aqueles cujas regras (R1) são aceitas.

Fonte: YDUQS

ACEITAR POR PADRÃO

Nesta política, todo o tráfego é autorizado, embora o destinado para determinados servidores seja negado.

Qualquer tráfego é aceito por padrão. Regras específicas (R1 e R2) definem quais serão negados.

Neste vídeo, conceituaremos a segurança física e a lógica, além do controle de acesso.

MÃO NA MASSA

1) (2019 - IF-BA - ASSISTENTE EM ADMINISTRAÇÃO) A RESPEITO DOS CONCEITOS QUE ENVOLVEM A SEGURANÇA DA INFORMAÇÃO, ANALISE AS AFIRMATIVAS A SEGUIR.

OS MECANISMOS DE SEGURANÇA PODEM SER LÓGICOS OU FÍSICOS.

A PERDA DE CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE É UM EXEMPLO DOS EVENTOS QUE COMPROMETEM A SEGURANÇA DA INFORMAÇÃO.

ASSINATURA DIGITAL, ENCRIPTAÇÃO E *FIREWALL* SÃO EXEMPLOS DE MECANISMOS LÓGICOS DE SEGURANÇA.

ASSINALE:

A) Se somente as afirmativas I e II estiverem corretas.

B) Se somente a afirmativa II estiver correta.

C) Se somente a afirmativa I estiver correta.

D) Se todas as afirmativas estiverem corretas.

2) (2019 - COMPERVE - UFRN - ANALISTA DE TECNOLOGIA DA INFORMAÇÃO) A SEGURANÇA COMPUTACIONAL POSSUI UMA TERMINOLOGIA PRÓPRIA. UMA PADRONIZAÇÃO NA UTILIZAÇÃO DESSA TERMINOLOGIA GARANTE O CORRETO ENTENDIMENTO ENTRE OS DIFERENTES AGENTES ENVOLVIDOS. EM RELAÇÃO A ISSO, CONSIDERE AS SEGUINTES AFIRMAÇÕES SOBRE A SEGURANÇA COMPUTACIONAL.

A SEGURANÇA FÍSICA VISA A PROVIDENCIAR MECANISMOS PARA RESTRINGIR O ACESSO ÀS ÁREAS CRÍTICAS DA ORGANIZAÇÃO A FIM DE GARANTIR A INTEGRIDADE E A AUTENTICIDADE DOS DADOS.

UMA AMEAÇA PODE SER DEFINIDA COMO ALGUM EVENTO QUE PODE OCORRER E ACARRETAR ALGUM PERIGO A ALGUM ATIVO DA REDE. AS AMEAÇAS PODEM SER INTENCIONAIS OU NÃO INTENCIONAIS.

SÃO AMEAÇAS MAIS COMUNS ÀS REDES DE COMPUTADORES O ACESSO NÃO AUTORIZADO, O RECONHECIMENTO (EX.: PORTSCAN) E A NEGAÇÃO DE SERVIÇO (EX.: DOS OU DDOS).

O “TRIPÉ DA SEGURANÇA” É FORMADO DE PESSOAS, PROCESSOS E POLÍTICAS DE SEGURANÇA. DE NADA ADIANTA UMA POLÍTICA DO TIPO SE AS PESSOAS E OS PROCESSOS NÃO FOREM CONSIDERADOS.

EM RELAÇÃO À SEGURANÇA COMPUTACIONAL, ESTÃO CORRETAS AS AFIRMATIVAS:

A) III e IV

B) II e IV

C) II e III

D) I e II

3) (2016 - CESPE /CEBRASPE - TRT - 8ª REGIÃO - ANALISTA JUDICIÁRIO - TECNOLOGIA DA INFORMAÇÃO) CORRESPONDEM A ITENS CAPAZES DE OFERECER CONTROLE OU PROTEÇÃO NO ÂMBITO DA SEGURANÇA FÍSICA PREVENTIVA:

A) As chaves públicas criptográficas.

B) Os dispositivos de autenticação biométrica.

C) Os sistemas de autenticação por senhas single sign on.

D) Os certificados digitais.

4) (2013 - FCC - TRT - 9ª REGIÃO - TÉCNICO JUDICIÁRIO – SEGURANÇA) CONVÉM QUE SEJAM UTILIZADOS PERÍMETROS DE SEGURANÇA (BARREIRAS, COMO PAREDES, PORTÕES DE ENTRADA CONTROLADOS POR CARTÃO OU BALCÕES DE RECEPÇÃO COM RECEPCIONISTAS) PARA PROTEGER AS ÁREAS QUE CONTENHAM INFORMAÇÕES E INSTALAÇÕES DE PROCESSAMENTO DA INFORMAÇÃO. ALÉM DISSO, QUE SEJAM LEVADAS EM CONSIDERAÇÃO E IMPLEMENTADAS AS SEGUINTES DIRETRIZES PARA PERÍMETROS DE SEGURANÇA FÍSICA, QUANDO APROPRIADO:

OS PERÍMETROS DE SEGURANÇA DEVEM SER CLARAMENTE DEFINIDOS, ASSIM COMO A LOCALIZAÇÃO E CAPACIDADE DE RESISTÊNCIA DE CADA PERÍMETRO PRECISAM DEPENDER DOS REQUISITOS DE SEGURANÇA DOS ATIVOS EXISTENTES NO INTERIOR DO PERÍMETRO E DOS RESULTADOS DA ANÁLISE/AVALIAÇÃO DE RISCOS.

OS PERÍMETROS DE UM EDIFÍCIO OU DE UM LOCAL QUE CONTENHA INSTALAÇÕES DE PROCESSAMENTO DA INFORMAÇÃO PRECISAM SER FISICAMENTE SÓLIDOS (OU SEJA, O PERÍMETRO NÃO DEVE TER BRECHAS NEM PONTOS ONDE PODERIA OCORRER FACILMENTE UMA INVASÃO).

DEVE-SE IMPLANTAR UMA ÁREA DE RECEPÇÃO OU OUTRO MEIO PARA CONTROLAR O ACESSO FÍSICO AO LOCAL OU AO EDIFÍCIO. ESSE ACESSO DEVE FICAR RESTRITO SOMENTE AO PESSOAL AUTORIZADO.

DEVEM SER CONSTRUÍDAS BARREIRAS FÍSICAS, ONDE FOR APLICÁVEL, PARA IMPEDIR O ACESSO FÍSICO NÃO AUTORIZADO E A CONTAMINAÇÃO DO MEIO AMBIENTE.

ESTÁ CORRETO O QUE SE AFIRMA EM:

A) II, III e IV

B) I, II e III

C) II e III

D) I, II, III e IV

5) AO PROJETAR UMA REDE, É COMUM ADOTAR UM FIREWALL PARA PROTEGER UMA REDE INTERNA. COM RELAÇÃO AO PAPEL DO FIREWALL, MARQUE A OPÇÃO QUE APRESENTA UMA FORMA CORRETA DE CLASSIFICAR ESTE ATIVO DE TIC.

A) Segurança lógica

B) Segurança física

C) Segurança patrimonial

D) Segurança empresarial

6) A PARTIR DA PANDEMIA OCORRIDA EM 2020, OS SISTEMAS DE ACESSO EVOLUÍRAM PARA O USO DE RECONHECIMENTO FACIAL. MUITOS DESTES SISTEMAS POSSUEM SLOGANS BEM CRIATIVOS, COMO ESTE: "UM SISTEMA DE ACESSO COM RECONHECIMENTO FACIAL PERMITE LEVAR A SUA EMPRESA DIRETAMENTE PARA O MUNDO DA ALTA TECNOLOGIA POR MEIO DO USO DESTA IMPORTANTE FERRAMENTA DE SEGURANÇA _______________".

MARQUE A ALTERNATIVA QUE APRESENTA O TERMO QUE COMPLETA O SLOGAN ANTERIOR DE FORMA MAIS SATISFATÓRIA.

A) Lógica

B) Física

C) Mista

D) Empresarial

GABARITO

1) (2019 - IF-BA - assistente em administração) A respeito dos conceitos que envolvem a segurança da informação, analise as afirmativas a seguir.

Os mecanismos de segurança podem ser lógicos ou físicos.

A perda de confidencialidade, integridade e disponibilidade é um exemplo dos eventos que comprometem a segurança da informação.

Assinatura digital, encriptação e *firewall* são exemplos de mecanismos lógicos de segurança.

Assinale:

A alternativa **"D "** está correta.

Mecanismos ou controles de segurança podem ser lógicos e físicos. A segurança da informação é baseada em três aspectos fundamentas: confidencialidade, integridade e disponibilidade. Desse modo, a perda de qualquer um dos três aspectos já impacta na segurança. A pior situação ocorre quando perdemos os três juntos: trata-se praticamente de uma catástrofe. Por fim, os mecanismos lógicos, por definição, envolvem algoritmos.

2) (2019 - Comperve - UFRN - analista de tecnologia da informação) A segurança computacional possui uma terminologia própria. Uma padronização na utilização dessa terminologia garante o correto entendimento entre os diferentes agentes envolvidos. Em relação a isso, considere as seguintes afirmações sobre a segurança computacional.

A segurança física visa a providenciar mecanismos para restringir o acesso às áreas críticas da organização a fim de garantir a integridade e a autenticidade dos dados.

> **Uma ameaça pode ser definida como algum evento que pode ocorrer e acarretar algum perigo a algum ativo da rede. As ameaças podem ser intencionais ou não intencionais.**
>
> **São ameaças mais comuns às redes de computadores o acesso não autorizado, o reconhecimento (ex.: PortScan) e a negação de serviço (ex.: DoS ou DDoS).**
>
> **O “tripé da segurança” é formado de pessoas, processos e políticas de segurança. De nada adianta uma política do tipo se as pessoas e os processos não forem considerados.**

Em relação à segurança computacional, estão corretas as afirmativas:

A alternativa **"C "** está correta.

A segurança é baseada em camadas; na parte física, são definidos os controles de acesso a determinadas regiões da instituição, como, por exemplo, cancelas, catracas e sistemas de acesso biométrico. Quando eles perdem sua finalidade, o atacante pode chegar fisicamente perto do equipamento, podendo danificar a parte física dele. Dos vários problemas que podem ser realizados, devemos destacar a possibilidade de se quebrar o equipamento (colocando em risco a integridade da informação) ou modificá-lo de forma prejudicial (colocando em risco a autenticidade da informação). Contudo, não podemos garantir esses fatores. Neste ponto um problema é gerado, pois ainda existem outros mecanismos que podem prover, pelo menos, a autenticidade dos dados.

A ameaça é um evento que pode provocar a perda de um dos três pilares da segurança: confidencialidade, integridade e disponibilidade. Sobre as ameaças comuns às redes, os exemplos estão corretos, porém, de acordo com as últimas estatísticas, isso pode mudar a qualquer momento. Tais ameaças são comuns, pois, até o presente momento, não existe uma solução completa para isso.

3) (2016 - CESPE /Cebraspe - TRT - 8ª Região - analista judiciário - tecnologia da informação) Correspondem a itens capazes de oferecer controle ou proteção no âmbito da segurança física preventiva:

A alternativa **"B "** está correta.

A segurança física está relacionada ao acesso às dependências das instalações; a lógica, aos algoritmos que protegem os dados.

4) (2013 - FCC - TRT - 9ª Região - técnico judiciário – segurança) Convém que sejam utilizados perímetros de segurança (barreiras, como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação. Além disso, que sejam levadas em consideração e implementadas as seguintes diretrizes para perímetros de segurança física, quando apropriado:

> **Os perímetros de segurança devem ser claramente definidos, assim como a localização e capacidade de resistência de cada perímetro precisam depender dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da análise/avaliação de riscos.**
>
> **Os perímetros de um edifício ou de um local que contenha instalações de processamento da informação precisam ser fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão).**
>
> **Deve-se implantar uma área de recepção ou outro meio para controlar o acesso físico ao local ou ao edifício. Esse acesso deve ficar restrito somente ao pessoal autorizado.**
>
> **Devem ser construídas barreiras físicas, onde for aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente.**

Está correto o que se afirma em:

A alternativa **"D "** está correta.

As instalações físicas devem possuir seguranças justapostas de forma que a fraqueza de uma camada possa ser recoberta por outra. Essa lógica fica clara no funcionamento de guaritas, cancelas e sensores biométricos.

5) Ao projetar uma rede, é comum adotar um firewall para proteger uma rede interna. Com relação ao papel do firewall, marque a opção que apresenta uma forma correta de classificar este ativo de TIC.

A alternativa **"A "** está correta.

O *firewall* é um importante ativo de rede; desse modo, encontrá-lo em um projeto de rede torna-se imprescindível. Ele protege uma rede interna analisando e bloqueando, por meio de algoritmos proprietários de cada marca, o acesso e o transporte de dados para dentro dela. Por manipulá-los,

este ativo é classificado como segurança lógica.

6) A partir da pandemia ocorrida em 2020, os sistemas de acesso evoluíram para o uso de reconhecimento facial. Muitos destes sistemas possuem slogans bem criativos, como este: “Um sistema de acesso com reconhecimento facial permite levar a sua empresa diretamente para o mundo da alta tecnologia por meio do uso desta importante ferramenta de segurança _______________”.

Marque a alternativa que apresenta o termo que completa o slogan anterior de forma mais satisfatória.

A alternativa **"B "** está correta.

Um sistema de acesso, independentemente do tipo de chave (senha) criado, permite o bloqueio físico a determinado local. Esta chave (senha), com o passar do tempo, vem evoluindo bastante: cartões com códigos de barra, tarja magnética, digital, veias da mão e, agora, reconhecimento facial.

GABARITO

VERIFICANDO O APRENDIZADO

1) (2019 - FCC - TRF - 4ª REGIÃO - ANALISTA JUDICIÁRIO - SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO) SUPONHA QUE UM ANALISTA DO TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO SE DEPARE COM UMA SITUAÇÃO EM QUE DEVE IMPLANTAR MECANISMOS DE PROTEÇÃO INTERNA VOLTADOS À SEGURANÇA FÍSICA E LÓGICA DAS INFORMAÇÕES NO AMBIENTE DO TRIBUNAL. PARA ISSO, ELE LEVANTOU OS SEGUINTES REQUISITOS:

NÃO INSTALAR EM ÁREAS DE ACESSO PÚBLICO EQUIPAMENTOS QUE PERMITAM O ACESSO À REDE INTERNA DO TRIBUNAL.

OS USUÁRIOS NÃO PODEM EXECUTAR TRANSAÇÕES DE TI INCOMPATÍVEIS COM SUA FUNÇÃO.

APENAS USUÁRIOS AUTORIZADOS DEVEM TER ACESSO AO USO DOS SISTEMAS E APLICATIVOS.

É NECESSÁRIO PROTEGER O LOCAL DE ARMAZENAMENTO DAS UNIDADES DE *BACKUP* E RESTRINGIR O ACESSO A COMPUTADORES E IMPRESSORAS QUE POSSAM CONTER DADOS CONFIDENCIAIS.

O ANALISTA CLASSIFICOU CORRETA E RESPECTIVAMENTE OS REQUISITOS DE I A IV COMO UMA SEGURANÇA:

A) Física, física, lógica e física.

B) Física, lógica, lógica e física.

C) Lógica, física, lógica e física.

D) Lógica, física, física e lógica.

2) (2018 - CESGRANRIO - TRANSPETRO - ANALISTA DE SISTEMAS JÚNIOR - PROCESSOS DE NEGÓCIO) PARA PROTEGER AS REDES DE DADOS, AS EMPRESAS CRIAM PERÍMETROS DE SEGURANÇA FORMADOS POR COMPONENTES QUE AVALIAM O TRÁFEGO DE INGRESSO E EGRESSO. O COMPONENTE QUE UTILIZA LISTAS DE CONTROLE DE ACESSO FORMADAS POR REGRAS QUE DETERMINAM SE UM PACOTE PODE OU NÃO ATRAVESSAR A BARREIRA É A(O):

A) *Firewall*

B) Proxy

C) DMZ

D) IPS

GABARITO

1) (2019 - FCC - TRF - 4ª Região - analista judiciário - sistemas de tecnologia da informação) Suponha que um analista do Tribunal Regional Federal da 4ª Região se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das informações no ambiente do tribunal. Para isso, ele levantou os seguintes requisitos:

> **Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do tribunal.**
>
> **Os usuários não podem executar transações de TI incompatíveis com sua função.**
>
> **Apenas usuários autorizados devem ter acesso ao uso dos sistemas e aplicativos.**
>
> **É necessário proteger o local de armazenamento das unidades de *backup* e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.**

O analista classificou correta e respectivamente os requisitos de I a IV como uma segurança:

A alternativa **"B "** está correta.

A segurança física está relacionada ao acesso às instalações, enquanto a lógica trata dos algoritmos.

2) (2018 - Cesgranrio - Transpetro - analista de sistemas júnior - processos de negócio) Para proteger as redes de dados, as empresas criam perímetros de segurança formados por componentes que avaliam o tráfego de ingresso e egresso. O componente que utiliza listas de controle de acesso formadas por regras que determinam se um pacote pode ou não atravessar a barreira é a(o):

A alternativa **"A "** está correta.

O *firewall* usa as regras para criar barreiras e políticas relacionadas.

CONCLUSÃO

CONSIDERAÇÕES FINAIS

Neste tema, elencamos os conceitos básicos da área de segurança e informação, citando seu valor, sua propriedade e seu ciclo de vida, além dos conceitos de segurança física, lógica e controle de acesso.

No módulo 1, abordamos o ciclo de vida e os problemas relacionados em cada etapa. Em seguida, apresentamos os principais mecanismos de segurança, como a criptografia, além destes pilares de segurança: confidencialidade, integridade e disponibilidade.

No módulo seguinte, falamos sobre a segurança física, que se relaciona com o acesso físico às instalações, e a lógica, que está ligada aos algoritmos. Também verificamos conceitos importantes, como o do *firewall* e das zonas delimitadas por ele.

Para ouvir um *podcast* sobre o assunto, acesse a versão online deste conteúdo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma ABNT ISO/IEC 27.0002/2013** – boas práticas para gestão em segurança da informação. Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BARRETO, J. dos S.; ZANIN, A.; MORAIS, I. S. de; VETTORAZZO, A. de S. **Fundamentos de segurança da informação**. São Paulo: Sagah, 2018.

BE COMPLIANCE. **Ladrão rouba HDs com dados de 29 mil funcionários do Facebook**. Publicado em: 19 dez. 2019.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal.

FREIRE, A. **Notebooks furtados da Petrobras estavam na Bacia de Santos, diz PF**. *In*: G1. Publicado em: 5 fev. 2008.

GUSMÃO, G. **Os 15 maiores vazamentos de dados da década**. *In*: Exame. Publicado em: 21 fev. 2014.

MEARIAN, L. **Survey**: 40% of hard drives bought on eBay hold personal, corporate data. *In*: Computerworld. Publicado em: 10 fev. 2009.

RODRIGUES, F. N. **Segurança da informação** – princípios e controles de ameaças. São Paulo: Érica, 2019.

EXPLORE+

Pesquise em canais do Youtube vídeos sobre:

IBM Cloud e Amazon Web Services: A nuvem ou *cloud computing* é um processo que vem mostrando muita força;

Supercomputador Santos Dumont: Como frisamos, ele é o maior recurso computacional do país. Conhecê-lo é uma ótima forma de analisar as medidas de segurança.

CONTEUDISTA

Anderson Fernandes Pereira dos Santos

CURRÍCULO LATTES